REMARKS

This is in full and timely response to the above-identified Office Action. The above listing of the claims replaces all prior versions, and listings, of claims in the application. Reexamination and reconsideration in light of the proposed amendments and the following remarks are respectfully requested.

Claim Amendments

In this response all of the pending claims have been cancelled and replaced with a new set (42- 56). This of course moots all of the rejections under §§§ 112, 101 and 103.

The newly presented claims have been cast in a manner which addresses the Examiner's concerns with respect to obviousness. The subject matter of original claims 5, 6, 8 and 11 has been incorporated into new independent claim 42.

The newly presented claims have been crafted to obviate the rejections under 35 USC § § 101 and 112.

The specification has been amended in accordance with paragraph #7 of the office action and the title suggested by the Examiner in paragraph #5, has been used. Sub-headings have been suitably introduced into the specification (see Substitute Specification) as per paragraph #6 of the office.

It is submitted that the newly presented claims distinctly define novel and inventive subject matter. More specifically, US 5,745,574 (Muftic) discloses a certification system for a public key infrastructure. The infrastructure can be hierarchical or in a matrix arrangement.

Referring to Figure 4 of Muftic and the accompanying description:

* U2 sends U1 a digitally signed message, in the example without a certificate.

* U1 then establishes whether or not the digital signature from U2 is valid by requesting certificates from U2, CA2 and CA3, verifying the certificates using the common point of trust CA1.

* Verification is achieved through checking signatures i.e. CA1 or signed CA2 certificate. Then, on the basis that CA2 can be trusted, the CA2 assigned CA3 certificate etc. is checked.

Once U1 has verified that it has a valid public key for U2, U1 then has to check that the key is authentic using a content digest.

To obtain a certificate, user U1 sends a certificate request message to each party from which it wishes to obtain a certificate (column 12, lines 11-13). The certificate request message is explained further with reference to Figure 25 (see column 17, lines 28-38).

Since Muftic relies on a cascade of authorizations, the certificate request message does not include any of the message received from U2. There is nothing in the disclosure of Muftic suggesting that any of the received messages is onward transmitted. In requesting a certificate, U1 is not requesting of CA2 or CA3 a certificate of U2 (hence U2 need not even be identified) but merely their certificates so that it can use these to verify a subsequent chain in the hierarchical structure.

Accordingly, even if the certificate transmitted from U2 to U1 can be regarded as a credential, the second party (U1) does not communicate to a third party at least one obfuscated credential from the composite credential.

It is submitted, therefore, that Muftic neither discloses nor suggests the feature of claim 1 which requires the second party to communicate "to a third party at least one obfuscated credential from the composite credential".

The reference to the "Handbook of Applied Cryptography" by Menezes is noted. However, while information can be derived therefrom, it is not seen that there is any "teaching" which might provide the allegedly obvious motivation to combine any of the

information that is disclosed with any teachings that can be gleaned from the disclosure of Muftic, in a manner that would arrive at the subject matter now claimed.

US 5,497,421 (Kaufman) et al discloses a password security system including "double encryption" which is described at column 9, lines 30-40, and also at column 4, lines 15-26. Both these sections disclose a single credential that is double encrypted, not different obfuscation for at least two credentials in a composite credential.

It is submitted, therefore, that Kaufman does not disclose the feature of claim 1 requiring different obfuscation to be used for at least two credentials in the composite credential. The same obfuscation is used in Kaufman, albeit in a two stage process.

Furthermore, it would be contrary to the teaching of Muftic for different elements of the certificate (Fig 3) to be encrypted using different obfuscation.

Conclusion

It is respectfully submitted that the newly presented claims overcome all of the objections/rejections which have been advanced in this Office Action and present subject matter which is allowable over the art applied. Favorable reconsideration and allowance of this application is therefore courteously solicited.

Respectfully submitted,

Date: 12/16/2005

By _____

HEWLETT-PACKARD COMPANY
Customer No.: 022879

William T. Ellis
Registration No. 26,874

Keith J. Townsend
Registration No. 40,358